Vragen? Opmerkingen? Tips? Mail ze naar brieven@clickx.be.

DOE HET ZELF

Brief van de week

De Clickx-redactie wordt elke dag overstelpt met vragen van lezers. Sommige problemen zijn te specifiek om in het magazine te behandelen, maar andere vragen zijn dan weer zo interessant dat ze meer verdienen dan een kort antwoordje. Daarom selecteren we voor elke Clickx Magazine een vraag van een lezer, die we dan uitwerken in een complete workshop. De vraag vind je op deze pagina, de workshop staat op de volgende twee pagina's. Veel plezier!

SCHIJF MET SLEUTEL

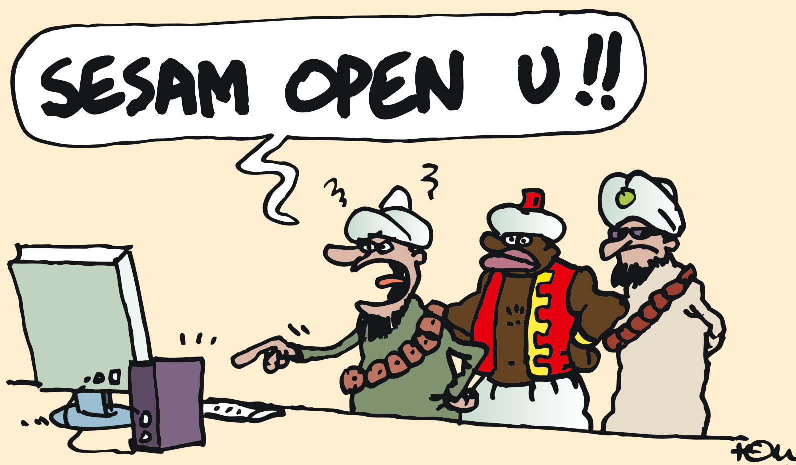


Hoe beveilig ik een externe harde schijf met een wachtwoord, zodat alleen ik er toegang tot krijg? Ik gebruik Windows XP.

PAUL VAN VLIET



Privacygevoelige gegevens scherm je natuurlijk graag af van spiedende oogjes. De beste manier om dat te doen, is door je gegevens te versleutelen en ze met een stevig wachtwoord af te schermen. In Windows XP Professional zit zo'n encryptiemechanisme ingebouwd – EFS of encrypting file system – maar Home-gebruikers grijpen naast de prijzenpot. Nu zijn er wel commerciële producten, zoals Hpsetool www.hexprobe.com (circa € 18, na gratis proef) of Cryptic Disk www.exlade.com (circa € 35, na gratis proef), maar waarom betalen als er ook een uitstekend gratis alternatief voorhanden is: TrueCrypt!





SCHIJF MET SLEUTEL



WAT DOEN WE?
- EEN EXTERN MEDIUM (ZOALS EEN HARDE SCHIJF OF USB-STICK) VERSLEUTELEN

WAARMEE?
- TRUECRYPT 4.3a

HOELANG?
- EEN KWARTIER

MOEILIJKHEID?

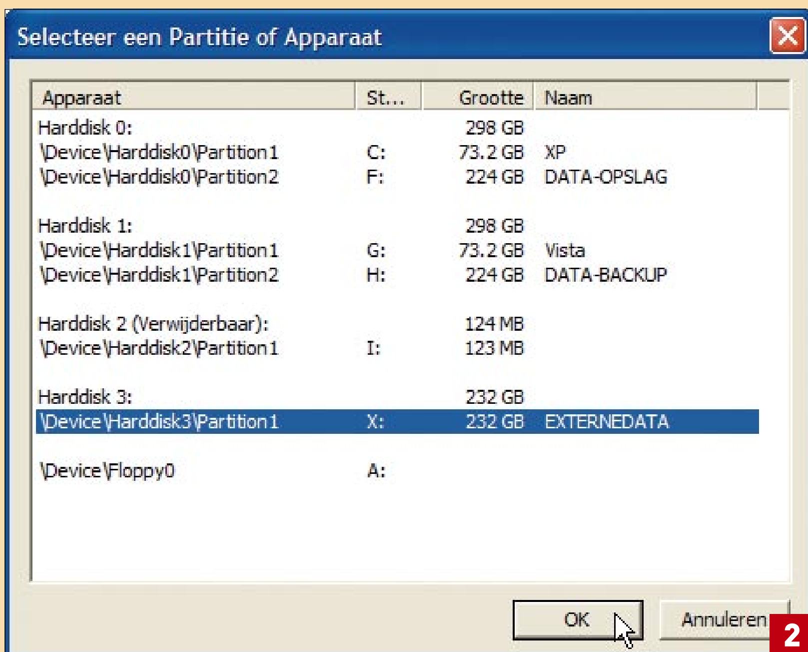


STAP 1 / DOWNLOAD & INSTALLATIE

Truecrypt, dat zowel onder Windows (XP, 2000, 2003 en Vista) als Linux draait, kan je downloaden van www.truecrypt.org. Op het moment dat we dit schrijven, was de laatste stabiele versie 4.3a. Na de download blader je meteen even door naar www.truecrypt.org/localizations.php, waar je terecht kan voor een Nederlands taalbestand. Heb je alles binnengehaald, pak dan het zip-bestand uit en start het uitvoerbare exe-bestand op. In principe mag je alle opties ongewijzigd laten en kan je dadelijk de **Install**-knop indrukken. Even later mag je de installatiewizard al verlaten. Over nu naar het taalbestand. Pak ook dit uit, en kopieer het bestand **Language.nl.xml** naar de installatiemap van TrueCrypt – standaard is dat \Program Files\Truecrypt. Nu ben je klaar om TrueCrypt op te starten (via **Alle programma's**, **TrueCrypt**). TrueCrypt lacht je al meteen in het Nederlands toe. Zoniet, dan vereist dat slechts een ommetje naar het menu **Settings**, waar je **Language**, **Dutch** aanklikt.

STAP 2 / STANDAARD VOLUME OP PARTITIE

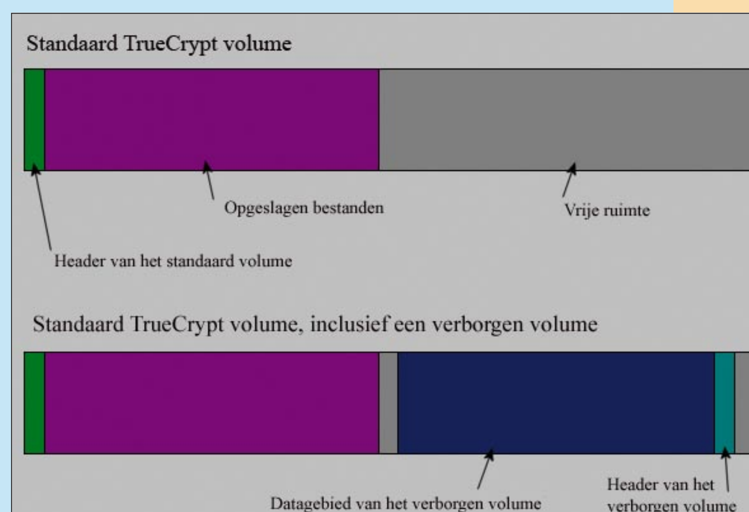
Om een schijf te versleutelen, druk je op de knop **Maak volume** in het hoofdvenster van TrueCrypt. Daarmee schud je een wizard wakker. In het eerste venster krijg je dadelijk een wat eigenaardige vraag op je bord: verkies je een standaard TrueCrypt-volume of een verborgen exemplaar? In ons kaderstukje geven we daarover tekst en uitleg. Hier houden we het echter bij de eerste optie: **Maak een standaard TrueCrypt volume**. Bevestig met **Volgende**. TrueCrypt vraagt je nu de locatie aan te geven van het te versleutelen volume. Je krijgt twee mogelijkheden: je kan ofwel een reuzengroot dummybestand creëren dat zich naar Windows toe als een eigen stationsletter zal voordoen, of je kan ervoor opteren de volledige schijfpartitie te encrypteren. Ga je voor de eerste methode, dan kan je dus ook nog onversleutelde gegevens op die schijf kwijt; in het tweede geval niet. Een wezenlijk verschil dus, maar de methode zelf is gelijklopend. Wij gaan hier voor de tweede optie, en klikken in het hoofdvenster van TrueCrypt op de knop **Zoek Apparaat** – en dus niet op de knop **Zoek Bestand**. Een nieuw venstertje opent zich, waar je het gewenste toestel of de gewenste partitie selecteert (zie afbeelding 2). Bevestig je keuze met **OK** en negeer de waarschuwing. Druk op **Volgende**.



Een versleuteld volume koppel je aan een bestand of een apparaat.

VERBORGEN VOLUME

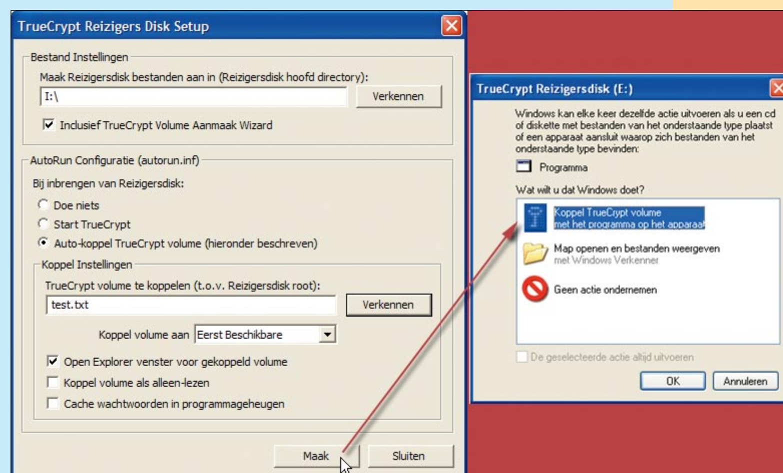
Je gegevens liggen veilig opgeslagen in een stevig versleuteld volume. Maar wat als iemand je op een of andere manier zou verplichten het wachtwoord prijs te geven? Ook daar heeft TrueCrypt een slimme oplossing voor bedacht: een verborgen volume! Zo'n volume wordt dan binnen een ander versleuteld TrueCrypt-volume gestopt. Dit buitenste volume voorzie je dan bijvoorbeeld van allerlei onschuldige gegevens, en je geeft het een ander wachtwoord mee dan je voor het verborgen volume had bedacht. Onder dwang kan je dan altijd nog dit wachtwoord – en dus dit buitenste volume – aan derden prijsgeven. Wil je echter toegang krijgen tot het binnenste, verborgen volume, dan moet je bij het koppelen van het buitenste volume het wachtwoord van het verborgen volume ingeven. Alleen dan geraak je ook dit volume binnen. Zonder dit wachtwoord is er niemand die ook maar een vermoeden kan hebben van je verborgen exemplaar – laat staan van de gegevens in dit volume!



Extra veilig: een versleuteld én verborgen volume.

SCHIJF OP REIS

Versleutel je een verwijderbaar medium (zoals een externe harde schijf of een usb-stick) met TrueCrypt, dan is het wel vervelend als je die ergens onderweg aan een andere computer hangt. Op die pc is TrueCrypt immers wellicht niet geïnstalleerd. Ook daar heeft TrueCrypt een oplossing voor... Na het aanmaken van zo'n volume (zie workshop, maar kies in dit geval wél voor een bestandscontainer) open je het menu **Tools** in het hoofdvenster van TrueCrypt en kies je **Reizigers Disk Setup**. Druk op de bovenste knop **Verkennen** en verwijs naar de hoofdmap van je externe medium. Stip **Auto-koppel TrueCrypt volume** aan, verwijs via de knop **Verkenner** naar het bestand dat je TrueCrypt-volume herbergt en selecteer bij **Koppel volume aan** bij voorkeur **Eerst Beschikbare**. Bevestig met de knop **Maak** en met **OK**. Sluit TrueCrypt vervolgens af. Zodra je nu de schijf of stick aan een pc hangt, zal TrueCrypt normaal gezien automatisch opstarten en kan je het versleutelde volume als een stationsletter benaderen, althans nadat je het wachtwoord hebt ingetikt.



Stop een TrueCrypt-volume in je zak.

STAP 3 / VERSLEUTELINGSALGORITME

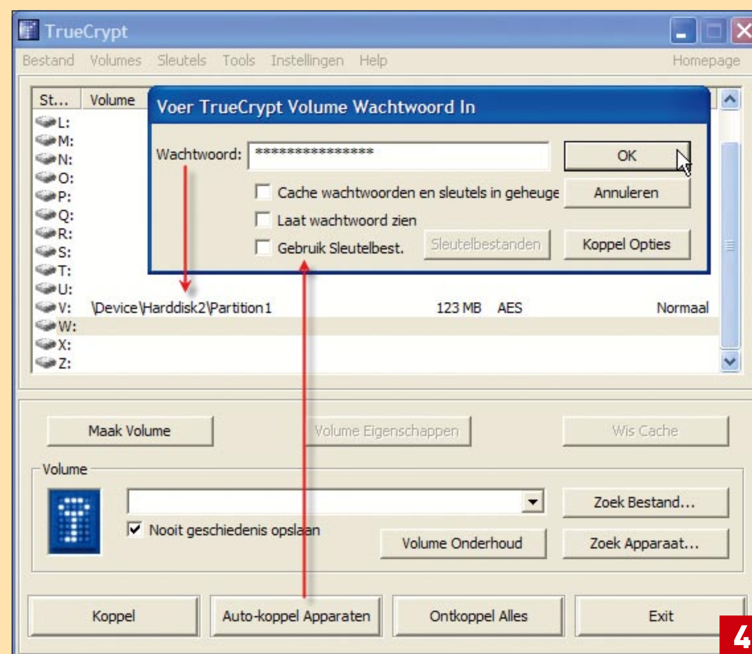
Het wordt nu iets technischer, met termen als coderingsalgoritme en hashalgoritme. Laat dat je echter niet tegenhouden, want de standaardinstellingen van TrueCrypt – met het ijzersterke AES-algoritme – kan je zonder meer aanvaarden (zie afbeelding 3). Druk gewoon op **Volgende**. Aangezien we een apparaat of partitie hadden gekozen – en geen bestand(scontainer) – kunnen we alleen maar nota nemen van de vastgestelde volumegrootte. Je mag dus nogmaals op **Volgende** drukken. Een belangrijk moment is de keuze van je wachtwoord. Het heeft namelijk weinig zin je gegevens met een uitgekiend algoritme te laten versleutelen als je die zelf met een miserabel wachtwoord afschermt. Een combinatie van cijfers en letters is dus aangewezen, en maak je wachtwoord zeker niet korter dan 8 tekens (TrueCrypt raadt zelfs 20 tekens aan). Bevestig met **Volgende**. In principe behoud je het aanbevolen bestandssysteem en ga je voor de standaard clustergrootte. Tijd voor een rondje muisdraaien: beweeg die gedurende een aantal seconden snel over het TrueCrypt-venster – zo bekom je een stevige encryptiesleutel. Druk vervolgens op **Formatteer**. Een waarschuwing van formaat duikt nu op: alle bestaande gegevens op die schijf(partitie) worden verwijderd! Wil je dat niet, dan maak je eerst een back-up, of je kiest in stap 2 alsnog voor een bestandscontainer. Na de formattering druk je op **OK** en op **Sluiten**.



AES: vergt méér dan een hacker om te kraken!

STAP 4 / STATIONSKOPPELING

Je mag nu TrueCrypt opnieuw opstarten. De schijfletter waarmee je oorspronkelijk naar je externe schijf verwees, mag je niet meer gebruiken. Probeer je dat toch, dan geeft Windows te kennen dat die schijf 'niet geformatteerd' is (ook op een andere pc trouwens)! In plaats daarvan selecteer je in het hoofdvenster van TrueCrypt een andere, vrije stationsletter. Vervolgens druk je op de knop **Auto-koppel Apparaten**, tik je je wachtwoord in en bevestig je met **OK** (zie afbeelding 4). Een alternatieve manier is dat je via **Zoek Apparaat** eerst naar je externe schijf speurt en vervolgens op de knop **Koppel** drukt. Je zal merken dat Windows je versleutelde volume meteen heeft herkend als de door jou aangegeven stationsletter. Je kan nu net als vroeger bestanden creëren, wijzigen, enzovoort. Wil je die gegevens weer ontoegankelijk maken, dan hoef je dit gekoppelde volume maar in het hoofdvenster van TrueCrypt te selecteren en op de knop **Ontkoppel** te drukken. ♦



Bij elke werksessie hoef je slechts één keer je wachtwoord in te voeren.